HCL MyXalytics

HCLSoftware

Security Trust Center Document

HCL has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the HCL website at www.hcl-software.com.

Table of Contents

List of Figures

Document Revision History

This guide is updated with each release of the product or when necessary.

This table provides the revision history of this Guide.

Version Date	Description
September, 2025	HCL_MyXalytics_v6.7_Security_Trust_Center_Document
July, 2026	HCL_MyXalytics_v6.8_Security_Trust_Center_Document

1 Our Commitment to Security & Trust

At HCLSoftware, we are fundamentally committed to earning and maintaining your trust. Security, privacy, and compliance are the foundation of our products. The HCLSoftware security strategy covers all aspects of our business, including corporate and organizational security policies, incident management and response, business continuity and disaster recovery, secure software development processes, and privacy.

This Trust Center provides a transparent overview of the principles and practices governing HCL MyXalytics, giving you the confidence to leverage our product for visibility and insights for your hybrid-cloud environments.

2 Introduction

The HCL MyXalytics platform is a unified reporting and predictive analytics solution designed to provide unparalleled visibility into IT systems and processes. MyXalytics provides a robust security posture designed to protect customer data, ensure service availability, and meet stringent compliance requirements.

This unified reporting and dashboarding software is an enterprise-ready solution that aggregates data from various IT tools to create insightful reports and dashboards. MyXalytics provides a consolidated view of IT operations, helping decision-makers optimize costs, reduce risk, and drive continuous operational improvements.

MyXalytics is designed as a platform where not only a unified view of the entire IT landscape is provided, but also predictive analytics and FinOps can be performed as actions where it can forecast capacity and generate cost optimization recommendations from the collected data.

2.1 Data Sources

- **User**: Concerning the data in the application or the project, user details are one of the sources of data which is analyzed by using cognitive services, and a relevant response will be provided. The response can be a direct solution or further prompting to understand the query better. HCL MyXalytics can respond in a simple textual response.
- **ITSM**: HCL MyXalytics processes data from IT Service Management (ITSM) tools like ticketing systems and service desks. This data includes information on incidents, service requests, problems, and changes. Analysis of this data helps in optimizing service delivery, predicting potential service disruptions, and improving efficiency by identifying recurring issues and bottlenecks.
- **FinOps**: MyXalytics integrates with public cloud billing APIs and on-premises resources management APIs to enable FinOps Cost visibility and Cost optimization features (Cloud Financial Operations). It ingests data on resource usage, cost, and billing from cloud providers (like AWS, Azure, and Google Cloud). The platform analyzes this data to provide insights into cost optimization, budget forecasting, and resource allocation. Security for FinOps data focuses on strict access policies and compliance to protect sensitive financial and operational information.
- **System/Database/App monitoring**: HCL MyXalytics collects and analyzes data from various monitoring tools for systems, databases, and applications. These data sources include metrics on CPU utilization, memory usage, network traffic, database query performance, and application response times. This enables proactive identification of performance degradation, resource bottlenecks, and system anomalies. Security protocols for this data ensure its integrity and prevent unauthorized access to the underlying infrastructure information.
- **Event management:** The product leverages event management data, which includes events and alerts from devices like Servers, Network devices, Databases and Applications. By aggregating these events HCL MyXalytics can analyze the event management efficiency.

- **Knowledge Base (Chatbot):** The MyXalytics AI Chatbot uses a Knowledge Base (KB) as a structured data source. The KB contains how-to articles, FAQs, troubleshooting guides, and policy documents that enable the chatbot to provide self-service responses and instant resolutions. All content entering the KB undergoes pre-ingestion safety checks before it is indexed or made available for retrieval.

2.2 AI and Foundation Models Integration

The platform integrates with leading AI providers to power automation:

- **Azure OpenAI**: Advanced LLMs for natural language understanding
- **HCL BigFix AEX:** Provides the chatbot module's AI safety controls

2.3 Chatbot Data Handling

Chat data constitutes the primary data processed and stored in connection with the MyXalytics AI Chatbot capability. This section describes how chatbot-related data is captured, processed, stored, and protected.

2.3.1 User Query Data

The chat data from the user comprises mostly the user query in plain text form. The user can type their query as part of the Chatbot interface, and the text is captured and processed by the MyXalytics AI core.

User queries are generally not expected to contain sensitive or critical data, but users may type anything as a query.

User queries are not extracted for profiling purposes but are kept in encrypted form for historical logs and to support service continuity.

A configurable disclaimer/banner is displayed within the chat interface to instruct users not to enter personal or sensitive information when interacting with the chatbot.

2.3.2 Chatbot Response Data

Chatbot response data comprises AI-generated replies to user queries. Responses can include textual answers, links to knowledge base articles, structured data summaries, and references to integrated systems.

Responses are reviewed through output filtering before being returned to the user, blocking sensitive terms, data leakage, or prohibited topics.

The chatbot does not autonomously trigger any actions in integrated systems without appropriate user confirmation or authorization workflows.

All chatbot sessions are logged for audit and traceability purposes.

2.3.3 Session Management

Idle user sessions are automatically terminated after a configurable inactivity timeout (default: 15 minutes) to mitigate the risk of unauthorized access from unattended sessions.

All session data is encrypted in transit using TLS 1.2/1.3.

2.3.4 Transparent Use Notification

MyXalytics maintains ethical transparency by ensuring users are clearly informed when they are interacting with an AI-powered feature.

The chatbot interface displays appropriate AI disclosure indicators, and the configurable disclaimer reinforces appropriate data handling expectations.

2.3.5 Security

We integrate security into every phase of the product lifecycle, from concept to deployment, to protect your data and infrastructure.

2.3.6 Secure by Design

HCL MyXalytics is developed in-house following a secure software development lifecycle. The product undergoes a comprehensive threat modeling assessment to proactively identify, evaluate, and mitigate potential security risks from the ground up.

- **Secure-by-Design Architecture**: Adheres to best practices for data encryption, access controls, and secure authentication mechanisms.

  Encrypted Transmission:

  - **Data at Rest:** All data stored is encrypted using AES-GCM 256-bit encryption, ensuring confidentiality and integrity at rest.
  - **Data in Transit**: As the portal shows summarized data to users it is transmitted over secure channels such as the TLS 1.2/1.3 mechanism.
- **Audit Logs & Role-Based Access Control**
  - Complete tracking of user and system activity ensures traceability and accountability.
- **Third-Party Component Vetting**:
  - All dependencies and libraries undergo rigorous vulnerability and license compliance checks.
- **AI/ML Infrastructure Isolation**
  - The predictive engine is architected using a containerized isolation model. Each analytical model serves within a dedicated containerized environment (e.g., Kubernetes), providing filesystem and process-level isolation. This prevents a vulnerability in one specific model from impacting the broader reporting infrastructure or the underlying IT data sources.

2.4 Secure Product Development

HCL Software adheres to stringent development processes to produce the code we develop and provide for our customers. All Development practices incorporate change control and are the key criteria assessed at release approval stage including key practices around following

Figure 1 –Secure Product Development

3 Requirements & Planning

- **Data Privacy Assessment**: HCL's Privacy and Data Protection by Design and Default (PbD) addresses privacy requirements during design and verification phases. HCL Software uses the One Trust Platform to perform Data Privacy assessments for products, platforms, and operations support.
- **Quality Planning and Certification**: A Quality Planning and Certification Deck is prepared with key quality metrics and is approved by the QA Lead.
- **AI Risk Assessment**: An AI-specific risk assessment is conducted for every major release to identify, categorize, and mitigate AI-related risks before deployment.

4 Design

- **Threat Modelling**: The process of identifying and prioritizing potential threats to a system and finding mitigation strategies.
- **Secure Design Review**: Conducted by the HCL Software Security team to assess product architecture, deployment methods, and existing security measures based on industry standards.

5 Development

- IDE-Level Code Linting
- Open-Source Code Composition and Vulnerability Analysis
- Static and Dynamic Application security testing
- Code Quality and Code Smell Analysis
- Penetration Testing: Internal penetration testing is done for every release, and external testing is conducted annually to find vulnerabilities that attackers could exploit.

6 Maintenance

- **Security Bulletins & Vulnerability Management**: The HCL Product Security Incident Response Team (PSIRT) manages the receipt, investigation, and internal coordination of reported security vulnerabilities for HCL Software product offerings.
- The PSIRT coordinates with product development teams who investigate reported vulnerabilities and identify the appropriate response plan. For more information, visit the HCLSoftware PSIRT page.
- The HCL PSIRT publishes Security Bulletins describing any relevant CVEs and pointing to additional details and remediation. A list of security bulletins for HCL MyXalytics can be found on the official HCL Software support and community forums.
- **Product Security Training**: Periodical training sessions are conducted for product teams on Secure Development, ISMS, Data Privacy, PSIRT Process, and more.

6.1 Secure distribution of binary:

- The binaries for the product are securely distributed via MHS Portal. My HCLSoftware (MHS) is a web application for HCLSoftware customers and partners that provides a new and improved way to find and quickly download the latest HCLSoftware product releases as well as supported older releases.
- All binaries are cryptographically signed. The system verifies signatures to prevent tampering.MHS provides seamless access to resources and tools designed to effectively manage the use of HCLSoftware products and services.
  - Access-controlled content: users only see content appropriate for them
  - Enables seamless access to resources and tools to help effectively manage the entire HCLSoftware experience

6.2 Data Privacy

- Data privacy (also called information privacy) refers to the right of individuals to control how their personal information is collected, used, shared, and stored. It's about ensuring that personal or sensitive data is handled in ways that protect people's rights and maintain their trust.
- In our relationship, the **customer is the data controller**, retaining full ownership and control over the data collected and determining the purpose of its use. For more information visit HCL Software Privacy

6.3 Purpose, Limitation, and Data Minimization

- The platform is designed to process personal data for the sole purpose of product administration and fulfilling our contractual obligations. We practice data minimization, and the product is not designed to process any special categories of sensitive personal data. Customer Information Processed: The platform may process the following customer information as part of its standard functionality:
  - Contact Information: Organizational Email Address
  - Personal Identification: First Name, Full Name, Last Name
  - User Account Information: Login ID

- Browsing Information - Session Time and IP Address
- Business Unit name/Company/Customer Name
- Conversation Chat Data: User queries and AI-generated responses from the chatbot, stored in encrypted form.

7 Responsible AI Controls

7.1 Human Resources Security

- Human resources security practices, background checks, and training processes are taken care of by the HCL Software team.
  - Risk management
    - HCL Software has a formalized risk management program that aligns with ISO 27034, ISO 31000 and ISO 27005 best practices, as well as ISO 27001/27002.
    - Risk management processes are integrated with other management systems, such as the Information Security Management System (ISMS). Security controls are implemented in accordance with our ISMS to manage risk across the organization.

7.2 Responsibility for Risk Management

- To drive the remediation of risks, our program reports risk status and escalates where necessary to senior management to inform business decision-making. Senior executives have overall responsibility as risk owners for mitigation, avoidance, transference, or acceptance of the risk. HCL Software uses a combination of weekly, monthly, and quarterly meetings and reports to ensure communication of risks.
- Every HCL Software staff member is responsible for the effective management of risk, including the identification of potential risks, the development of risk mitigation plans, and the implementation of risk reduction strategies.

7.3 AI Risk Management

- HCLSoftware has defined processes and procedures for managing and accessing information systems and operational security risks. HCL MyXalytics undergoes regular assessments to identify and assess the likelihood and impact of risks. These potential risks include unauthorized access, use, disclosure, or disruption to HCL MyXalytics systems and customers. Risks are categorized in accordance with a formally documented procedure.
- Any identified risk is managed in a timely manner to safeguard the confidentiality, integrity, and accessibility of HCL MyXalytics systems and customer data.

8 GEN AI Data Security & Responsible AI Controls

- MyXalytics takes a defense-in-depth approach to securing Generative AI systems, covering user data, model interactions, infrastructure, and ethical governance.

8.1 User Data Protection

- **Encryption in Transit and at Rest**: All user inputs, outputs, and metadata are encrypted using TLS 1.2/1.3 for data in transit and AES-256 for data at rest.
- **Zero Retention of Sensitive Inputs**: User prompts or responses classified as sensitive are not retained unless explicitly required and approved by the customer.

8.2 Access Control & Identity

- **Role-Based Access Control (RBAC)**: Fine-grained access is enforced to ensure only authorized users can interact with or configure AI services.
- **Single Sign-On (SSO) & SAML 2.0 Integration**: Federated identity ensures authenticated access aligned with enterprise identity providers.
- **Audit Logs**: All access and activity logs are captured and monitored for suspicious behavior.

8.3 API & Model Access Security

- **API Key Management**: API keys are securely generated, rotated, and stored in secure manner using AES-256 encryption.
- **Scoped Access**: APIs are protected with least-privileged permissions and rate-limiting to avoid abuse or overuse. Public facing APIs are hosted behind the API gateway with rate limiting.
- **Defender for Cloud**: Continuous security posture management with Azure Defender for Cloud (or similar services) ensures compliance, threat detection, and remediation for AI workloads.

8.4 Content Filtering & Prompt Validation

- **Real-Time Content Filtering:** Built-in content moderation checks for toxic, harmful, or restricted content are applied before generating any output.
- **Prompt Injection Protection (Summarization)**: Report titles, entities, and numbers are fed to the model as controlled artifacts — not as user-controlled context. Prompts that set the AI context are not exposed to or modifiable by users.
- **Prompt Injection Protection (Chatbot):** Input screening and pattern detection are applied to identify and block prompt injection and jailbreak attempts.
- **Output Filtering:** Sensitive terms, data leakage, or prohibited topics are blocked before responses reach the user.
- **Knowledge Safety Controls:** Content entering the retrieval pipeline is reviewed and safeguarded before being used in AI responses. Retrieved content is treated as untrusted input.

- **Runtime Safeguards:** Input and output guardrails enforce scope, confidentiality, and safe response behavior during AI execution.

8.5 Secure Development Practices

- OWASP for GenAI: Regular testing is conducted against OWASP Top 10 for Large Language Models (LLMs), including:
  - Prompt injection
  - Model denial-of-service (DoS)
  - Insecure plugin design
  - Sensitive information disclosure
  - Inadequate sandboxing
  - Supply chain vulnerabilities
- **Defender for Cloud:** Continuous security posture management ensures compliance, threat detection, and remediation for AI workloads.
- **Comprehensive Security Testing:** Covers threat modelling, SAST, DAST, dependency scanning, and container image scanning.
- **Strict Environment Separation:** Dev / Test / Production environments are strictly separated with least-privilege access controls.

8.6 Responsible AI and Ethical Safeguards

- **Explainability & Auditability**: All AI outputs are traceable with logs and rationales for key decision-making.
- **Human-in-the-Loop Review**: Product is using Gen AI models for text summarization only and no actions are triggered based on the model response. Prompts for summarization are reviewed before they are enabled on the production.

8.7 AI Governance & Risk

- **AIMS scope and policy:** Follows HCLSW AI policy and scope for the AI Management System (AIMS) with defined accountable roles and hu man oversight for safety-critical use cases.
- **AI risk register**: Risk register covering model theft, inference leakage, and over-reliance risks.

9 Secure MLOps Lifecycle Management

9.1 Data Sourcing & Preparation

- Access control to data sources via RBAC
- Automated data provenance and lineage tracking

Data poisoning prevention through schema validation and anomaly detection**Model Training**

- Encrypted communication for distributed training nodes

Adversarial robustness testing to pre-empt evasion attacks**Model Deployment**

- All deployments containerized with minimal base images
- Deployment policies enforce runtime security constraints

9.2 Model Governance

9.2.1 Model Lifecycle Management

- **Version control:** Tracking different versions of models, datasets, and features.
- **Lineage tracking:** Recording data sources, transformations, training parameters.

9.2.2 Data Governance

- **Data quality monitoring:** Checking for missing, corrupt, or skewed data.
- **Data lineage:** Traceability from raw sources to model inputs.
- **Privacy compliance:** Ensuring privacy is respected (e.g., through anonymization, consent logging).

9.2.3 Model Explainability & Interpretability

- Use of integrated model-specific explainers.
- Model Cards

9.2.4 Fairness & Bias Monitoring

- Pre- and post-deployment bias checks across attributes (gender, race, etc.).
- **Fairness metrics**: e.g., equal opportunity difference, demographic parity.

9.2.5 Model Performance Monitoring

- **Drift detection:** Concept and data drift.
- **Performance degradation tracking**: E.g., AUC, F1-score over time.

9.2.6 Auditability & Traceability

- **Comprehensive logging**: Who trained what, when, using which data and parameters.
- **Audit trails:** For external compliance and internal accountability.

9.2.7 Access Control & Security

- **RBAC**: Role-based access control on models and datasets.

- Model encryption and secure deployment.
- Secure APIs and access tokens for inference.

9.2.8 Retraining & Lifecycle Refresh

- Triggered by performance decay or data drift.
- Appropriate role needed for retraining.
- Tracking retraining logic, triggers, and audit logs.

9.2.9 Compliance and Certifications

- The HCL MyXalytics platform has the following compliance certifications/attestations available:

9.2.10 ISO 27034

- FinOps Certified Platform
  - HCL MyXalytics is recognized as a FinOps Certified Platform, supporting cloud cost visibility, allocation, optimization, budgeting, forecasting, and governance practices aligned with FinOps principles.
- FinOps Certified Practitioner
  - The MyXalytics team includes FinOps Certified Practitioners who bring validated FinOps knowledge and expertise to help customers adopt best practices for cloud financial management, cost accountability, and optimization.

10 Conclusion

Our valued clients can rest assured that we keep security foremost in our minds as we develop, test and deliver effective and secure reporting and analytics solutions to our customers. For more information, please contact us

HCLSoftware

hcl-software.com